WHAT IS CLAIMED IS:

1. A method of identifying service abuse, comprising:

receiving an event requesting a service;

creating an event identification associated with the event;

incrementing a count value of a first table entry of a plurality of table entries in a screening table in response to the event identification matching an event identification associated with the screening table entry;

decrementing a count value of a selected table entry of the plurality of table entries in response to the event identification failing to match an event identification associated with the selected table entry;

replacing the selected table entry with the event identification associated with the event in response to the count of value of the selected entry equaling zero; and

determining a metric value for the event from the screening table, the metric indicating that the event is an abusive request.

2. The method of claim 1, wherein the event identification corresponds with the identity of a user.

3. The method of claim 2, wherein the event identification includes an IP address.

4. The method of claim 2, wherein the event identification includes a user identification.

5. The method of claim 1, wherein the event identification corresponds with a content value included in the event.

6. The method of claim 5, wherein the content value includes at least a portion of a message.

7. The method of claim 5, wherein the content value includes at least a portion of a URL.

8. The method of claim 1, further including:

selecting a second table entry as a new selected table entry in response to receiving the event.

9. The method of claim 1, further including:

selecting a second table entry as a new selected table entry in response to the event identification failing to match an event identification associated with the selected table entry.

10. The method of claim 1, further including disregarding the event in response to the metric value crossing a threshold value.

11. The method of claim 1, further including terminating a connection used to receive the event in response to the metric value crossing a threshold value.

12. The method of claim 1, further including returning an error message in response to the event in response to the metric value crossing a threshold value.

13. The method of claim 1, further including:

determining an average metric value from the metric value and a set of previous metric values; and

disregarding the event in response to the average metric value crossing a threshold value.

14. The method of claim 1, wherein determining a metric value comprises:

determining a first sub-metric value from the screening table;

determining a second sub-metric value from a second screening table;

determining the metric value from a weighted combination of the first and second sub-metric values.

15. A system for identifying service abuse, comprising:

a plurality of server computers each adapted to receive an event and to create an event packet in response to the event;

a cluster host adapted to receive a plurality of event packets from at least a portion of the plurality of server computers and to update a master screening table in response to the plurality of event packets; and

wherein the cluster host is further adapted to communicate a local screening table comprising at least a portion of the master screening table to each of the plurality of

server computers, and each of the plurality of server computers is adapted to disregard an event matching a portion of the local screening table.

16. The system of claim 15, wherein the local screening table is a copy of the master screening table.

17. The system of claim 15, wherein each event packet includes an event identification associated with a event.

18. The system of claim 17, wherein the event identification corresponds with the identity of a user.

19. The system of claim 18, wherein the event identification includes an IP address.

20. The system of claim 18, wherein the event identification includes a user identification.

21. The system of claim 17, wherein the event identification corresponds with a content value included in the event.

22. The system of claim 21 wherein the content value includes at least a portion of a message.

23. The system of claim 21, wherein the content value includes at least a portion of a URL.

24. The system of claim 21, wherein the content value is a hash of the content value included in the event.

25. The system of claim 15, wherein the cluster host is further adapted to determine a metric value for an entry of the master screening table, the metric indicating that the entry of the master screening table corresponds to an abusive request.

26. The system of claim 25, wherein the cluster host is further adapted to set a block value associated with the entry in response to the metric value.

27. The system of claim 25, wherein the cluster host is adapted to determine an average metric value from the metric value and a set of previous metric values and to set a block value associated with the entry in response to the average metric value.

28. The system of claim 15, wherein the cluster host is adapted to determine a first sub-metric value from the entry, to determine a second sub-metric value from an entry of a second master screening table, and to determine the metric value from a weighted combination of the first and second sub-metric values.